6. Information Distribution

This chapter includes core network applications common to all users including electronic mail, web services, file transfer, and directory services. The relationship of this chapter with the ITSG is shown in Figure 6-1.

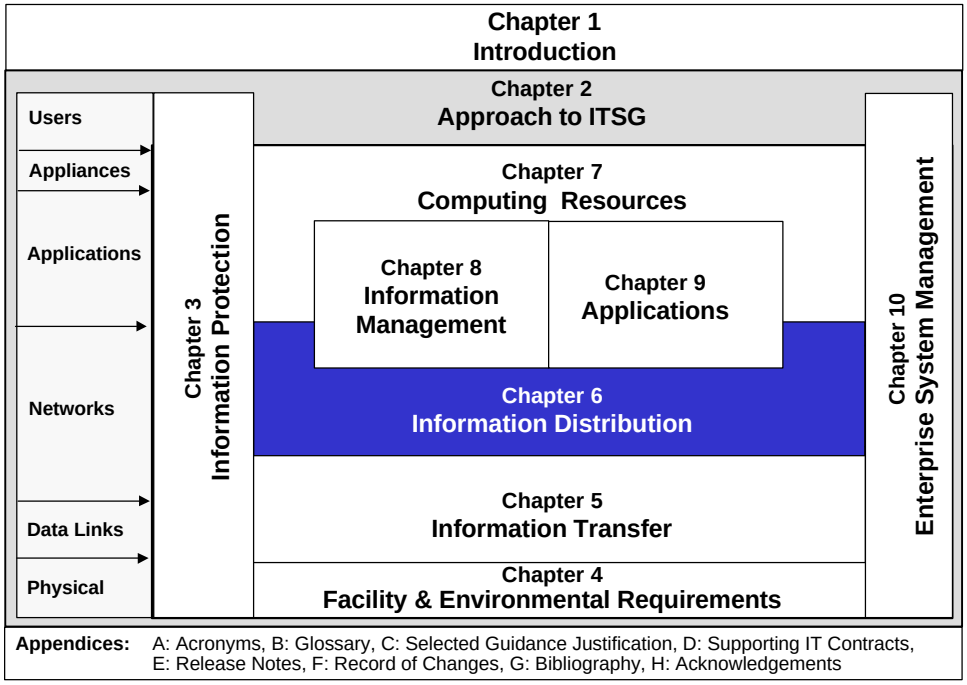

Figure 6-1. ITSG Document Map Highlighting Chapter 6, Information Distribution

6.1 Overview

Information distribution is effectively the "nerve center" of the information technology paradigm. As shown in Figure 6-1, information distribution is the nexus of information protection, information transfer, computing resources, information management, applications and enterprise system management. It is the zone where communication technologies meet computer processing technologies. Where in the past both of these technologies had their separate cultures, information distribution brings these two cultures together enabling a new, more comprehensive and effective information technology culture.

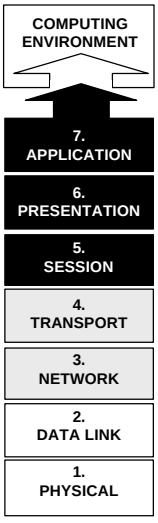

Figure 6-2. ISO/OSI Model Layers 5 - 7+

Whereas Chapter 5, Information Transfer, focused on the first four layers of the International Standards Organization/Open Systems Interconnect (ISO/OSI) seven layer model, Chapter 6, Information Distribution, extends the Transport and Network layer and completes the last three layers, Session, Presentation, and Application, into the computing environment (Figure 6-2).

The term "information distribution" is short for a more descriptive term: Basic Network and Information Distribution Services (BNIDS). BNIDS organizes the network and provides fundamental applications that all users in all functional

areas require. BNIDS includes the configuration of the network and network devices to establish node, user and device identification, system domain establishment, a routing or switching schema to move information to its final destination, security services, directory services, electronic mail (e-mail) including attachments, electronic dialog (chat), and web services (http). Figure 6-3 summarizes BNIDS by using the standard ITSG method of placing the foundation technologies on the bottom and working toward the user at the top.

As shown in Figure 6-3 Figure 6-3, there are 13 items that will be described in order. The concept of operations provides the context in which all BNIDS technologies fit together to give the user an integrated product.

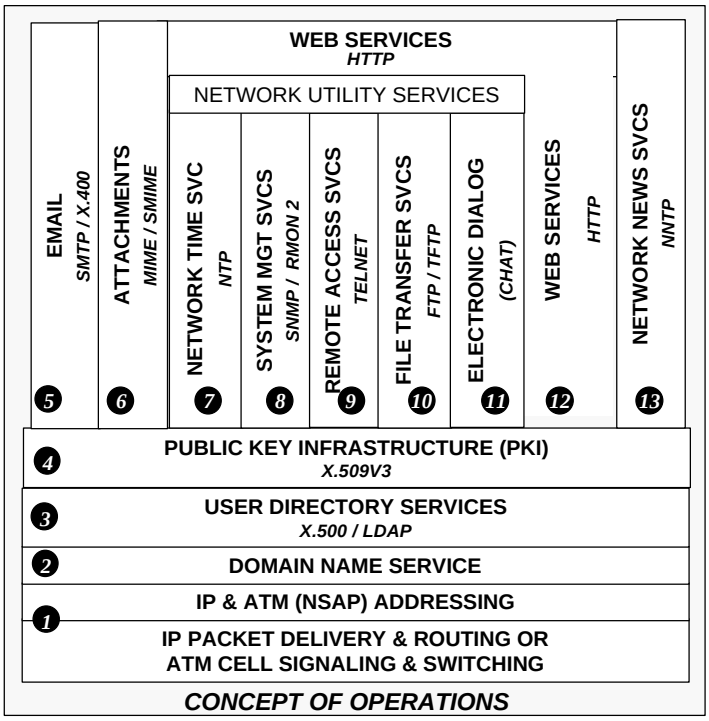

Figure 6-3. Basic Network and Information Distribution Services (BNIDS) Showing the Order of Discussion

The five technologies at the bottom are pervasive to all of the BNIDS and support the upper level technologies.

IP Packet, Delivery, IP Addresses, ATM Cell Delivery and NSAP Addresses are all information transfer technologies covered in Chapter 5.

Domain Name Service (DNS) allows people to specify network device addresses in more friendly (human readable) terms.

User Directory Service allows any system or user of the information infrastructure to find the electronic office or mail home of another person or organizational entity.

Public Key Infrastructure supports protection of information content during transfer across the network thereby supporting need-to-know among trusted users. It also provides a trusted login server to support greater accessibility with adequate protection.[5]

The nine technologies shown in Figure 6-3 as vertical columns are specific to particular functions that are common to all users and system devices.

Electronic Mail (e-mail) permits transfer of messages between users, organizational entities, and groups of users.

Attachments allow attaching files in any media to an e-mail message. These attachments can be documents, programs, sound bites, animations, video clips, entire videos, etc.

Network Time Service permits synchronization of clock time among the many system devices that have to interact across the network. Each device has minute variations in clock speed that accumulate over time and can potentially affect operations (e.g., a "future time late" because of a time-stamp from a source clock that is faster than a destination clock).

System Management Services goes beyond remote access in that it provides a set of standard protocols that allow monitoring, collection of data and control of the system devices.

Remote Access Services support logging into remote computers and network devices from distant management centers to primarily perform administrative tasks. This feature supports centralized management of distributed devices but inherits a significant security risk that must be mitigated through other means.

File Transfer Service permits the direct push or pull of information files (any media) from one computer to another.

Electronic Dialog allows real-time (or near-real-time) conversations to occur over the network. Normally this service is associated with teletype 'chat' which uses relatively low bandwidth and is useful for troubleshooting over links with small data rates. It does not include voice, telephone and video teleconferencing services because these services demand relatively high bandwidth and are not available to all users (tactical and non-tactical).

Web Services allow users to traverse the network to various information sources through a network ("web") of objects (words, pictures, icons, etc.) linked to other files and information sources.

Network News Services allow creation and sustainment of electronic, interactive bulletin boards to support a running dialog or notice of current events, status, direction or debate.

The standards and guidance associated with Figure 6-3 and the preceding summary of BNIDS will be expanded through the rest of this chapter. First, a BNIDS concept of operations is described, followed by amplifying sections on domain name services, directory service, public key infrastructure, e-mail and attachments, network utilities, and web services. The e-mail section

[5] A complete description of Public Key Infrastructure (PKI) is provided in Chapter 3, Information Protection. Accessibility is a metric discussed in Chapter 10, Enterprise Management.

includes a detailed DON implementation strategy. The web services section provides valuable guidance on this rapidly emerging technology.

6.2 Concept of Operations for BNIDS

Command, Control, Communication, Computers, and Intelligence (C4I) for the Warrior, Copernicus, Information Technology for the 21st Century (IT21), and Marine Air Ground Task Force (MAGTF) C4I are similar system integration strategies that focus on tailoring the information infrastructure to support the common user. For BNIDS, the user is the warfighter, operator, marine or sailor. The user is the focus of the concept of operations.

6.2.1 Official Individual Accounts

Figure 6-4 depicts the user-centric focus on the officer, enlisted, and civilian as the critical component of all DON organizational structures. As discussed in Chapter 2, the DON is a very dynamic environment because of individual assignment rotations, embarking commands, and force movements. For Navy and Marine Corps, this environment renders as unsuitable many of the structures and protocols directed at the commercial world.

Official individual e-mail accounts help to address this dynamic situation. To enhance mission effectiveness, every individual in the DON will have an official account with an associated e-mail address. The individual will maintain his or her information system identity wherever they go during their Naval career. Individuals will be allowed to choose their own official e-mail address within some liberal formatting constraints. The individual e-mail address will be less than twelve characters in length. Nicknames, call signs, last names, first names will all be acceptable so that individuals gain a sense of ownership of their information system identities. The e-mail address can be put on business cards without requiring a change of cards upon command reassignment. Official individual business, such as detailing, fitness reports, and promotions can be conducted using the official individual account. The official individual account will always be on the unclassified part of the infrastructure, and changing an individual address will be allowed but not encouraged.

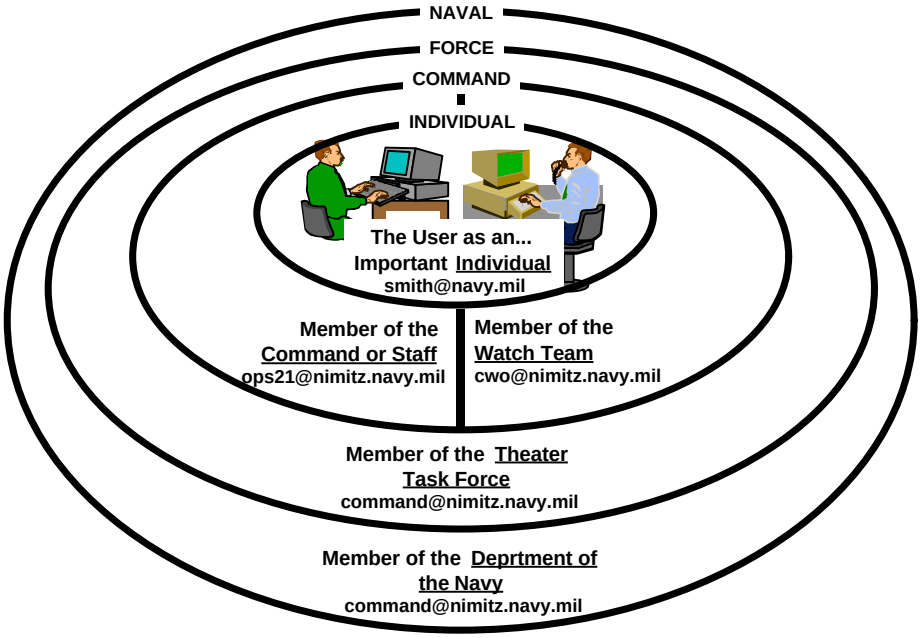

Figure 6-4. User-Centric View

Because it will be assigned to the Navy or Marine Corps system domain, the user's official individual account will move with the individual to a new assignment but remain unchanged. For example, a marine and a sailor are shown in Figure 6-4. The marine's name is GSGT Jones and the sailor's name is Petty Officer Smith. Jones has selected "jones" for his e-mail address and Smith selected "smith". Jones' full Simple Mail Transfer Protocol (SMTP)[6] e-mail address would be "jones@usmc.mil" and Smith's would be "smith@navy.mil"[7]. Each individual's official office account will reside on his/her command's file server either at the command itself or at the servicing Information Technology Service Center (ITSC)[8]. Upon transfer, the individual's official account will be transferred to the ITSC closest to the individual's next command where he or she will continue to receive e-mail and conduct official business (including family correspondence). The ITSCs will provide a 90 day transfer account to allow a graceful transition from the old to the new command. Again, the concept calls for Smith, Jones and all DON members to keep their official individual account throughout their career, wherever they are, even during transfer periods.

6.2.2 Command/Staff Accounts

As a member of the command or staff, each individual must also maintain an identity associated with the organization. For this, individuals would also have staff or command accounts with an identity associated with the command position or staff code. Unlike the official individual account, the command or staff account is rigidly formatted so that the command identity remains consistent, independent of the individual that holds the position. The individual may have as many as three command/staff accounts corresponding to the Unclassified, Secret and potentially

[6] SMTP was chosen because of its pervasiveness on DISN and the Internet and that it is presently more portable than X.400. This is described in the e-mail standards guidance provided in Section 6.5.

[7] The Information Technology Service Center would ensure that their names are unique within their domain.

[8] See Chapter 10 for a full description of the Information Technology Service Center (ITSC) concept.

Sensitive Compartmented Information (SCI) classification systems. To support this concept, each command and staff must establish staff codes or command positions to have an identity on the information infrastructure. (For example, “MPA” for Main Propulsion Assistant would have an account name and e-mail address of MPA@shipname.navy.mil.)[9]. Users can have their official individual e-mail forwarded to their command/staff account by the ITSC. This will be allowed and encouraged. Users could have their command/staff e-mail forwarded to their official individual account if there is a rational requirement, but generally, this practice will be discouraged.

6.2.3 Duty/Watch Accounts

Another command/staff virtual identity that must be represented in the information infrastructure is the duty or watch team. Members of the duty or watch team rotate daily but the command identity remains constant and is often the most critical position of the staff or command. As individuals assume the staff position they also assume ownership and all attendant responsibilities associated with the watch account. This watch identity is shown on Figure 6-4 in the right side of the command circle. Forwarding of official individual e-mail or command/staff mail will not be permitted.

6.2.4 Command Correspondence and Distribution Lists

Until Defense Message System (DMS) becomes fully operational, the following concept can be used to conduct command correspondence using SMTP. For command correspondence, each command will have an e-mail address of “command@command_name.navy.mil” for unclassified e-mail and “command@command_name.navy.smil.mil” for classified e-mail. “Command” in this case is a special account where e-mail from “command@command_name.navy.mil would have official command intent, direction, or information dissemination as provided by the Commanding Officer or his designated representative with command correspondence release authority. The Commanding Officer would still have a command/staff account (co@command_name.navy.mil) as well as his official individual account for his command and individual e-mail (e.g., co’s_lastname@navy.mil). E-mail delivered to “command@command_name.navy.mil” will be forwarded to an internal distribution list determined by the commanding officer or chief of staff. An anticipated distribution for “command@command_name.navy.mil” could be the duty officer, the executive officer, and a message profiler application that will forward the mail based upon key words in the text of the message itself. The use of a distribution list for expeditious delivery of command correspondence is extremely valuable. Other distribution lists could be used for special circumstances such as cat@command_name.navy.mil for a Crisis Action Team (CAT), or ato@command_name.navy.smil.mil for Air Tasking Order (ATO) planning. Members of the command, assisted by the ITSC, would manage these distribution lists. Mixing user names and command names on command correspondence e-mail is permitted. As in JANAP 128 record messages, the “To” line to designate “action required” versus the “Cc” line for “information purposes” should be maintained. Proper process dictates that the command/staff accounts should be receive-only, to ensure that originators of messages can be properly identified.

[9] Examples used in this section use the Navy’s domain for consistency. For all “navy.mil” examples, “usmc.mil” could be substituted for the same intent.

6.2.5 Directory Services

An enterprise directory service is required to track official individual accounts, command/staff accounts, duty/watch accounts, and distribution lists. This task would be challenging enough if the managed entities were not in a constant state of flux, as they are in the Navy and Marine Corps. The server that the user accesses to retrieve and send mail, as well as to conduct normal office automation tasks is referred to as his home account. (The home account can be referred to as a user's "mail home".) The home account moves at the discretion of the command or the user in the case of transfer or long term temporary duty. Commands or command elements that embark or deploy take their home accounts with them. Official individual home accounts would likely not move during embarkations or deployments but command/staff, watch accounts, and distribution lists would move.

Tracking and promulgating the location of the home account-e-mail address pairs would be the responsibility of X.500 *master directories* maintained by both the Navy and the Marine Corps to service each classification level (Secret Internet Protocol Routing Network (SIPRNET) and Non-classified Internet Protocol Routing Network (NIPRNET)). These master directories would be maintained at a central location with at least one backup at an alternate location. The master directory would likely be maintained by an ITSC which would serve as an X.500 source directory. There would be X.500 replication directories at each fleet teleport, and alternate locations determined by the Marine Corps, and in the San Diego region for performance and reliability. The Navy and Marine Corps X.500 directories would be linked with the Coast Guard's X.500 directory for full maritime coverage. Home account servers will employ the Lightweight Directory Access Protocol (LDAP) to access the X.500 source or replication directories to carry as much of the full X.500 directory as they need to perform their mission (Figure 6-5). Ships and tactical commands with limited communication bandwidth need to update their e-mail directories while in port or in garrison prior to getting underway or deploying.

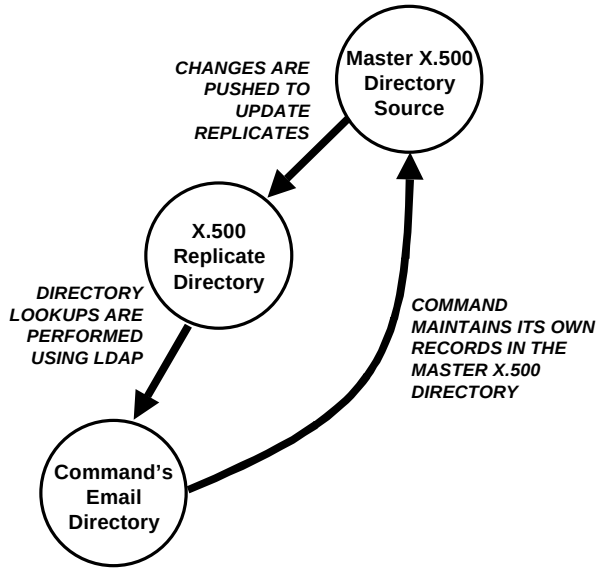

Figure 6-5. X.500 Directory Update and Maintenance

The Command Information Officer (CIO) should be established as the member of the command to coordinate with the ITSC to update the Navy or Marine Corps Master X.500 Directory (MXD).

Either the Command's CIO or the user will be able to update his own official individual record. Only the Command's CIO (or the Commanding Officer's designated officer) will be able to update command/staff accounts and command distribution lists. In all cases, commands will be responsible for maintaining their records in the Master X.500 Directory.

6.2.6 Defense Message System (DMS) Interoperability

DMS will become the official message delivery system in the DoD. The concept for DMS is to replace the aging Automatic Digital Network (AUTODIN) with an open standards-based system comprised of commercial products. DMS is based upon the X.400 e-mail standard and X.500 directory standard with special military alterations to meet the Required Operational Message Capability (ROMC). The DMS concept calls for the replacement of command-to-command formatted messages with writer-to-reader messages and multi-media attachments. Each individual message delivery would be protected through encryption and decryption of each message using Fortezza PC cards at the user's personal workstation. Messages would be either individual traffic (analogous to personal e-mail) or organizational traffic (analogous to the command correspondence concept described in Section 6.2.4 above).

Figure 6-6 illustrates this concept. A parallel design should also be used to support the SCI DMS requirements. As shown there are two DON DMS users, one on each fleet; there are two Navy SMTP-only commands, one on each fleet; and there is a cloud representing the community of DMS users in the DOD as well as a cloud representing the SMTP users in DoD. Seven cases of e-mail delivery are shown. All Navy and Marine Corps DMS traffic flows through one or more of the three MFI mail switches. DMS traffic flowing internal to the DON can use X.400 or a protocol employed by the mail switches and associated User Agents installed at the DMS user site's DMS server suite. DMS messages delivered outside of the DON will be translated to DMS-standard X.400 for subsequent delivery. The MFI mail switch will also receive DMS X.400 messages and commercial X.400 messages and translate them to SMTP for further delivery to any Naval command. All Naval commands, DMS or not will use SMTP to ensure tactical and tactical-support communication. Table 6-1 summarizes the DON interoperability with DMS.

To interface elements of the DON's dynamic environment that require SMTP e-mail with DMS that requires X.400 (e.g., for tactical and tactical support implementations), at least three sets of mail switches should be employed to serve as DMS Multi-Function Interpreters (MFIs). A set of mail switches will involve a pair of mail switches, one on the NIPRNET and one on the SIPRNET to maintain a consistent architecture on both the Secret and Unclassified networks. The three mail switch sets should be distributed as follows: one for the Marine Corps, one for the Atlantic Fleet and one for the Pacific Fleet. These MFI mail switches will support delivery of DMS traffic within the DON as well as to other DOD organizations.

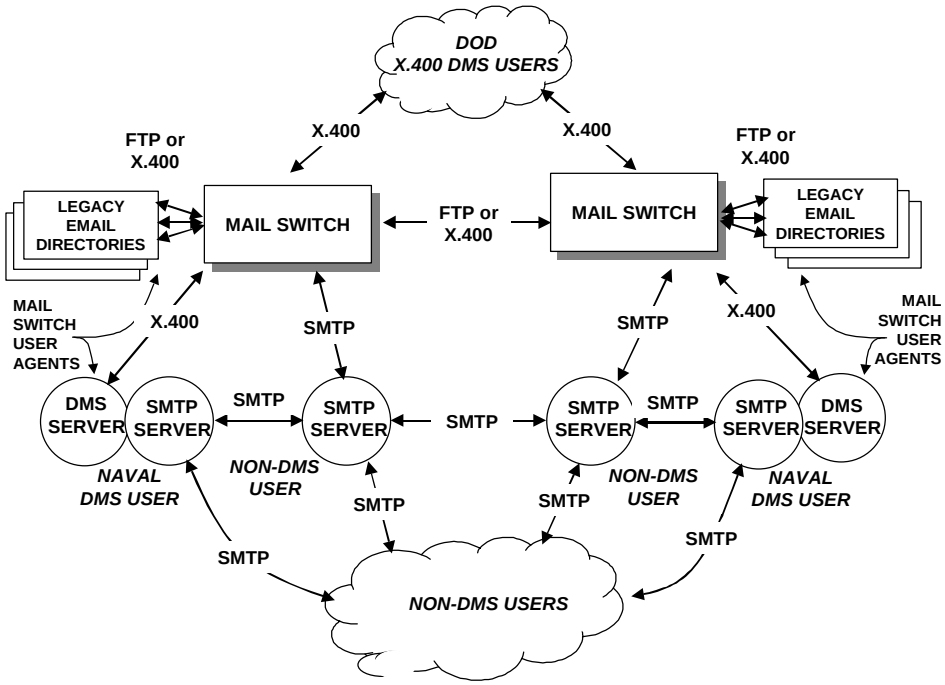

Figure 6-6. DMS Multi-Function Interpreters

		Path Description	
From	**To**	**Link**	**Protocol**
Navy DMS Site	SMTP Site	Navy DMS to MS MS to SMTP Site	X.400 SMTP
SMTP Site	Navy DMS Site	NA	Not Applicable. DMS only receives from authorized DMS sites.
Navy DMS Site	Navy DMS Site	Navy DMS to MS MS to MS MS TO Navy DMS	X.400 X.400 X.400
Navy DMS Site	DOD DMS Site	Navy DMS to MS MS to DOD DMS	X.400 X.400
DOD DMS Site	Navy DMS Site	DOD DMS to MS MS to Navy DMS	X.400 X.400
DOD DMS Site	Navy SMTP Site	DOD DMS to MS MS to Navy SMTP	X.400 SMTP
Navy SMTP Site	DOD DMS Site	NA	Not Applicable. DMS only receives from authorized DMS sites.
SMTP Site	SMTP Site	No gateways or interpreters	SMTP

Note: For above, MS means Mail Switch

Table 6-1. Interim DMS Interoperability with the DON Information Infrastructure

6.2.6.1 Directory Synchronization Side Benefit of the DMS MFI

A side benefit of the mail switch is that some products also translate native legacy e-mail directories into standard X.500. This feature should be acquired and used to maximize e-mail interoperability to all e-mail users as an interim measure until they can employ a X.500/LDAP based e-mail system. The mail switch could be used as a backup to the Master X.500 Directories. As changes occur through time, various e-mail directories will become outdated if subsequent updates are not made to the Master X.500 Directory. To minimize this effect, mail switch's directory synchronization capability can be used to automatically update outdated directory information. This occurs as commands with ownership of accounts change their directories; the mail switch will automatically detect and promulgate the changes to other participating e-mail servers.

6.2.7 Security Certificate and Login Services

To support information content and need-to-know protection, X.509v3 digital security certificates will be used to provide secure web connections (through Secure Socket Layer (SSL)) and encrypted e-mail attachments (through Secure Multipurpose Internet Mail Extension (S/MIME)). A complete description of the Public Key Infrastructure (PKI) used to support Security Certificate and Login Services is provided in Section 3.5. PKI could support a common login server that would manage secure connections to the multitude of applications, information bases and servers that a user must traverse to collect required information in a network centric world. Rather than remembering a unique account and password for every server or application encountered, servers and applications would maintain a trusted relationship with the login server who would provide the necessary security parameters while the user collects the required information. At this time, establishing a common login server is too risky to pursue at the DON enterprise level but additional security using SSL and S/MIME is very beneficial. Security certificate authorities should be established and managed across the DON to appropriately support both fleet and shore based activities The certificates and certificate revocation lists should be stored in the Master X.500 Directories. The official DON policy for implementation of PKI is provided in Section 3.5.

6.2.8 Web Drop and Pickup Service

Web Drop and Pickup (WDP) service offers an alternative method to e-mail attachments to transfer large files (e.g., greater than 2 MB). A WDP Server must be established either at a servicing ITSC or at one of the commands involved in the file transfer. The sender of the large file uploads the file to the WDP Server then sends an e-mail message to the intended recipients with the hyperlink or instructions on how to fetch and download the file. This service improves information management efficiency by allowing the recipient to download the large file at his convenience and when he has the bandwidth to do so (e.g., on the road with a slow speed modem). Additionally, the file does not consume the recipient's internal disk space if he decides that he does not need it. The network is less burdened by "pushed" attachments that are not necessarily needed. The sender is comforted to know that his attachment was less likely to cause an unintentional "denial-of-service" on his recipients through clogging their e-mail channel.

6.2.9 BNIDS CONOPS Summary

A concept has been presented that supports the following operational requirements:

- Official Individual Accounts And E-mail Addresses Held During An Individual's Entire Career
- Command/Staff User Accounts and E-mail Addresses
- Watch Accounts and E-mail Addresses
- Home Accounts/Mail Homes
- Command Correspondence
- Command Distribution Lists
- Individual Transfer Between Duty Stations
- Embarkation And Disembarkation of Highly Mobile Commands
- Directory Services Including Downloads, Updates, and Maintenance
- Interoperability With DMS
- Directory Synchronization
- Digital Security Certificates for Secure E-mail Attachments and Secure Web Links
- Web Drop and Pickup Service

This concept provides the context in which standards and guidance is provided for each of the BNIDS technologies to follow.

6.3 Domain Name and Directory Services

Naming and directory services are needed to locate resources on the network. These services provide the means for identifying and retrieving information about objects on the network. An object is a specific resource on the network such as a computer, application, file, e-mail box, printer, or router. Information that can be retrieved about an object varies according to the object and the name or directory service providing the information.

Naming and directory services are related in the functions they provide, but distinct differences exist. A naming service locates and retrieves information about an object solely by the name of the object. There are stand-alone systems, such as Internet Domain Name Service (DNS), that implement a naming service. However, most are integrated within other services, such as file systems and e-mail. Examples of integrated naming services are the name and address books within Lotus Notes, MS Exchange, and NetWare's file services.

In a directory service, each object is identified and retrieved based on its attributes, where one of the attributes is its name. This service provides the additional capability of searching for all objects that have one or more particular attributes — for example, "What are the names of all DON employees located in Crystal City?"

A new method of combining multiple directories, called meta-directories, is evolving. Meta-directories provide application-specific agents that synchronize the application directories (e-mail and operating systems) into a standard directory with access via the Lightweight Directory Access Protocol (LDAP).

6.3.1 Domain Name Service (DNS)

DNS translates computer host and network device IP addresses into understandable names and visa versa. It uses TCP/UDP as a transport service when used in conjunction with other services. The DON domains for NIPRNET are navy.mil and usmc.mil; for the SIPRNET it is navy.smil.mil and usmc.smil.mil.

A consistent, globally unique naming and addressing scheme is the key element in successfully implementing client/server applications and environments. This naming scheme is required for the objects being stored in directory systems. The names of the objects need to be logical and meaningful to the system users and to other applications. A name needs to conform to four specific principles:

- Alphanumeric, clearly conveying the built-in meaning
- Unique within its domain
- Not overly encoded or hexadecimal, except for security purposes
- Names and addresses of network entities must be globally unique to construct enterprise networks

Best Practices

Domain names for commands should be short but understandable abbreviations of the command name. The primary domain name for ships is the type and hull number with no dash, space or

punctuation in between. The ship name shall also be available as a domain name as an alias. Ships named after people should use only the last name for brevity. Where two ships are named after a distinguished individual with the same last name, at least one of the domain names should have the initial of the first name or enough of the first or middle name to attain a unique domain name. Use of commonly understood initials of the dedicated individual is also acceptable as a domain name of the ship (e.g., JFK, FDR). Shore commands shall use an abbreviation of their administrative name as the primary domain name rather than the task force designation. Commands with a permanent task force designation can have an alias domain name with the task force designation. Domain names for command attachments shall use the standard command domain name with the detachment designation directly appended with no space, underscore or dash.

The Network Information Center (NIC) requires that all DNS Servers have at least one secondary DNS at a remote location. For ships the primary DNS will be ashore at its servicing fleet teleport; its secondary will be aboard the ship.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DNS	DNS	DNS	DNS	DNS SEC
Activities, Platforms, Operational Environments		All			

Table 6-2. Naming Services Standards

Notes:

- The protocol for DNS is defined in Internet Engineering Task Force (IETF) Request for Comment (RFC) 1035.
- WINS (RFCs 1001, and 1002) is a Microsoft Windows 3.11, Windows 95, and Windows NT standard now widely used. However, Microsoft plans to migrate to Active Directory (AD) so WINS users should include plans for migration to AD in 1999 and beyond.
- DNS is IAB Standard 13, as profiled by MIL-STD-2045-17505

Examples:

USS Los Angeles:	ssn688.navy.mil and alias losangeles.navy.mil
USS Theodore Roosevelt	cvn71.navy.mil and alias tr.navy.mil or roosevelt.navy.mil
COMARFORLANT	cmfl.usmc.mil
USS City Of Corpus Christi	ssn705.navy.mil and alias cityofcorpuschristi.navy.mil
Commander ASW Forces Pacific	cafp.navy.mil and alias ctf12.navy.mil
COMCRUDESGRU FIVE	ccdg5.navy.mil

6.3.2 Directory Service

Best Practices

Use a two-tiered directory structure as defined within the Distributed Computing Environment (DCE). For local references, use a Cell Directory Service (CDS) and connect multiple local services to a Global Directory Service (GDS). GDS is implemented using X.500 (ISO 9594) or the Internet DNS. To enhance application portability in an environment implementing multiple directory technologies with diverse naming conventions, use X/Open Federated Naming (XFN) and Lightweight Directory Access Protocol (LDAP) as the access mechanism. LDAP has become a de facto standard as it is currently supported, or planned to be supported, by most electronic messaging and Web enabled applications.

Applications that have requirements for a full function directory service will conform to the X.500 directory standards. Applications that require a naming service should select a naming system that integrates with a directory (X.500) system.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	X.500 LDAP	X.500 LDAP	X.500 LDAP	X.500 LDAP	
Activities, Platforms, Operational Environments		All			

Table 6-3. Directory Service Recommended Implementations

Notes

- X.500 is the leading standard for directory services.
- The X.509 standard (the ITU recommended standard for Digital Certificates) should be fully supported in any selection of an X.500 directory system.

- Select an X.500 directory system and schema that are compatible with the DMS X.500 directory.
- Implementations should support interfaces from multiple network applications.
- LDAP access to the directory must be provided and it should be compatible with and accessible from popular e-mail clients.
- Directory updates can be very bandwidth intensive. Ships with limited bandwidth should always update their directories the day prior to getting underway.
- Directories should be maintained at multiple teleports to ensure proper service level for ships transiting different ocean areas.

Guidance

Most vendors support interoperable solutions for directory services and naming. While most directory data used today reside in integrated, vendor proprietary messaging and file systems, the transition to an X.500 environment with access via LDAP is the preferred implementation. As long as the back-end X.500 directory system is scaleable, most systems that implement LDAP as the access technology are sufficient.

Much thought needs to be given to how the directory schema is created and how the distributed directory server architecture is implemented. Refer to the DMS X.500 Directory Service Implementation Guidance (Draft) which provides the Schema, the policies and procedures for implementing the DMS Directory Service, as well as other information including the management of the directory service and the functions required to ensure an effective directory service.

Given the complexity and time frames associated with the DMS directory, it is recommended that DON maintain its own enterprise directory. Initially, this directory might be used to hold basic personnel information (e.g. Command, address, phone number) but would also be used to keep track of individual's SMTP addresses. This directory should be implemented using X.500 standards and be accessible via LDAP capable (e.g. Web browser) clients. An implementation of the directory would likely have multiple, fully replicated instances, and be located at strategic DON points of presence. Collocation with ITSCs would be a logical option. The directory service that currently exists at "directory.navy.mil" provides a good example of how the directory might be organized.

It is recommended that individuals be given the capability to access and update their individual records and that organizations be given the ability to perform "bulk" uploads and/or changes if necessary. Most commands and organizations will maintain their own directories for the purpose of resolving internal resource lookups, so complete or partial replication of the DON directory into these local directories should be made possible. The DON directory should also provide the mechanism to store X.509 v3 certificates as necessary for certain personnel.

For messaging, many systems have the ability to create and maintain an X.400 Originator/Recipient (O/R) address for all recipients in the MHS. This address identifies a mailbox recipient in the global X.400 (DMS) address space. The following table displays those X.400 attributes that should minimally be associated with DON electronic mailbox recipients in a directory.

X.400 Attribute	MHS Value
County (C)	US
Administrative Domain(A)	“ “ (blank)
Private Mgmt Domain(P)	ORGANIZATION
Organization (O)	ORGANIZATION
Organizational Unit (OU)	(e.g., NAVSEA, CINCLANT)
Common Name (CN)	TBD
Generational qualifier (Q)	TBD
Initials (I)	Initials
Surname (S)	Last Name
Given name (G)	First Name
Domain-defined attributes	TBD

Table 6-4. X.400 Address Attributes

6.4 Public Key Infrastructure (PKI)

A public key infrastructure is a collection of components that support the generation and distribution of digital certificates, issuance of certificate revocation lists (CRLs), and the building and running of directories to serve these certificates and CRLs. In order to understand the operational issues and to develop the proper policies associated with operating a PKI, a number of Naval, DoD, and other government entities are operating PKI pilot projects based on commercial standards. These pilots are called “medium assurance” PKI pilots based upon the level of assurance postulated in the digital signatures associated with the certificates. The Defense Message System (DMS) project is fielding a separate PKI based partially on commercial standards and partially on DMS unique standards (this pilot project is sometimes called a “high assurance” PKI).

A digital certificate is an electronic proof of identity that can be used to sign electronic documents, to authenticate the holder of the certificate, and to allow decryption of information intended to be read by the holder of the certificate. Digital certificates are used in many commercial products (e.g., SSL for WWW security, S/MIME for e-mail security) and are based on the use of public key cryptography. In a public key cryptographic system, a person (e.g., using a web browser) generates a public key/private key pair. The private key is never revealed to anyone and is protected by the application that generated it (in our example, the browser). The public key can then be published (e.g., in an X.500 database). It should be noted that PKI identities should also account for the use of command/staff e-mail accounts.

A complete description of PKI and associated standards guidance is provided in Section 3.5.

6.5 Electronic Messaging and Attachments

Electronic mail (e-mail) message handling systems (MHS) are integral to enterprise computing strategies. E-mail implementation for the Navy and Marine Corps must conform to both the Simple Mail Transfer Protocol (SMTP) and to the international e-mail messaging (X.400) for compliance with DMS. The e-mail implementation strategy must also maintain enterprise connectivity of dissimilar e-mail message handling systems until they can be migrated to a common standard.

A Message Handling System is the name of a methodology to exchange electronic messages between originators and recipients. Both SMTP and X.400 are implementations of an MHS. An originator is an entity (i.e. a person or computer program) that sends or originates a message. The recipient is another entity, a person or a computer program, that receives the message. Certain requirements should be satisfied when providing a message exchange service between an originator and recipient.

- The message must not get lost or be altered in transit. In order to ensure this, MHS defines the transfer rules according to which the message is passed from one messaging switch or entity to another messaging switch or entity.
- The handling entities must be able to interpret the message. This includes the originator and the recipient, as well as the message switches handling the message in transit, which need to route the message and perform tasks relevant to the transmission of the message.

Most good message handling systems should be able to provide more than these basic minimum features. For example, the originator may wish to know when the recipient receives the message. In this instance, the originator might require that they be notified if the recipient cannot receive the message, because, for example, the address specified by the originator was erroneous. These MHS features or capabilities are commonly referred to as service elements.

SMTP and X.400 share a number of common service elements, most of which are duplicated and extended in vendor proprietary MHS. In fact many vendor proprietary systems utilize either SMTP or X.400 as a baseline upon which they add additional service elements.

Standard Messaging Application Program Interfaces (MAPIs) provide access to directory services, message profiling, message store-and-forward capabilities, and electronic transport capabilities of message handling systems. A message type called X.435, present in the 1988 version of X.400, provides standardized support for Electronic Data Interchange (EDI) transaction transport and interchange over communications networks. This EDI message type facilitates the movement, delivery, and security of EDI transactions over X.400 networks.

To date, the interfaces between the DMS architecture and other related DON efforts involving messaging, such as IT21, have not yet been defined. For example, DMS has selected X.400 and X.500 for messaging and directory protocols while most of the industry is trending towards SMTP and LDAP. A “flexible architecture” approach for DMS implementation has tentatively been established to address these issues. A concept for the DON DMS flexible architecture has been proposed to establish the originally designed DMS application installed in the DII and within the DON infrastructure (Section 6.3). Other efforts could interface to this backbone to relay command messages and e-mail to commands (including ships, aircraft, submarines, mobile tactical units, and small shore commands). Existing COTS based software would allow for exchange of mail between the core DMS protocols (X.400/X.500) and Flexible Architecture Protocols (SMTP/LDAP).

The ultimate goal is to have a convergence in the tools that the DON uses to perform messaging. However, a distinction is necessary between the notion of “command correspondence” (e.g. JANAP 128 for GENSER or DOI 103 for SCI) and “personal messaging.” This distinction is primarily one of doctrine and procedures on how the messaging system is used versus the technologies used to construct the messaging system.

Best Practices

Choose electronic message handling systems that conform to Internet based (SMTP) standards as well as the international e-mail messaging (X.400). The chosen e-mail message handling systems should add Application Program Interfaces (APIs) to the basic e-mail message handling system services such as message store-and-forward and electronic transport.

For DMS compliant organizational messaging, products should be chosen that support the DMS standards. Messaging that requires elements of service unique to the DOD will use X.400 (DMS) protocols. Examples of such services include guaranteed delivery, timely delivery within tight time constraints, auditing, and alternate routing capabilities.

Secure Multi Purpose Mail Extension (S/MIME) is the preferred encoding for attachments. S/MIME requires use of an established Public Key Infrastructure (PKI) for issuing and revoking security certificates. Use of MIME is acceptable until a DON enterprise PKI is established. Because many of the most critical communication links are bandwidth limited, users should compress attachments whenever possible. ZIP 2.04 (or higher version) compression protocol should be used to compress all attachments.

Commercial versions of DMS compliant messaging systems should be selected for electronic messaging solutions and should be interconnected with SMTP and X.400. Messaging that requires only minimum essential elements of service would comply with a standards profile based on SMTP/S/MIME, LDAP, X.509(V)3, and IMAP-4 client to server interface standards. These standards likely address the majority of messaging needs throughout the DON. Post Office Protocol (POP3) services must continue to be provided until a transition to IMAP4 is complete.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SMTP X.400 (1992) POP 3 IMAP 4 MIME RFC 1521 S/MIME RFC2312 ZIP 2.04	SMTP X.400 (1992) POP3 IMAP 4 MIME RFC 1521 S/MIME RFC2312 ZIP 2.04	SMTP X.400 (1992) IMAP 4 MIME S/ MIME RFC 1521 ZIP 2.04	SMTP X.400 (1992) IMAP 4 MIME S/ MIME RFC 1521 ZIP 2.04	X.435 ESMTP
Activities, Platforms, Operational Environments		All			

Table 6-5. E-mail with Attachments Recommended Implementations

6.5.1 Implementation Guidance

- Select suppliers who support X.400, SMTP and the capability to handle compound documents between them.
- Support for the Multipurpose Internet Mail Extensions (MIME) and the Secure Multipurpose Internet Mail Extensions (S/MIME) standards should be included in any MHS solution.
- Post Office Protocol 3 (POP3) and International Mail Access Protocol (IMAP) do not constitute fully functional MHS, however POP3/IMAP access to a robust messaging solution may be appropriate in some situations. Choose an MHS that supports both standards now, but plan to phase out POP3 in favor of IMAP when practical.
- Avoid non-X.400-compliant messaging systems in 1999 and beyond. Explore the use of ESMTP when it becomes available.
- Products should, whenever possible, use X.500 for all naming and directory services and must support the Lightweight Directory Access Protocol (LDAP) standard for directory access.
- Select suppliers who have scaleable and manageable SMTP solutions that comply with IAB STD 10 (including RFC 821, SMTP, and the service extensions identified in RFC-1869 AND 1870).

6.5.2 Selection of an E-mail System

A handful of vendors have “enterprise class” solutions that can support organizational (i.e. DMS) as well as interpersonal electronic messaging. Using products available on the DMS contract, a significant number of DON customers have already made their e-mail system selection. In order

to reduce the cost and complexity of supporting different e-mail systems within a command, it is desirable to select an e-mail product that can address both the organizational and interpersonal messaging requirements. In addition, it is also prudent to be aware of the e-mail systems already selected by other DON commands – system homogeneity will facilitate communication with other DON commands. As with any other complex system, e-mail system selection should follow the guidance provided in section 2.9. Along with command functional requirements, DON wide security and seamless interoperability are two other overriding factors to be considered. Because it is a foundation technology that forms the core of DON Information Distribution, e-mail system homogeneity will be a driving factor in the push to reduce complexity and Total Cost of Ownership (TCO) within the DON. It is worth reiterating that care should be taken when selecting e-mail products that do not support both personal and organizational e-mail and where this decision deviates from mainstream DON products.

6.5.3 E-mail System Implementation

The requirement for DON e-mail systems to seamlessly interoperate suggests that the ITSG should provide guidance so that implementations throughout the Navy and Marine Corps are consistent and realize the full benefit of system features. The network operating system used to support the e-mail system implementation should be configured to support maximum flexibility and portability within the DON. It is desirable that commands moving between satellite footprints and those commands embarking aboard ships have continuous and seamless access to their resources (e.g. accounts, printers, and servers). This will necessitate significant DON collaboration on network operating system naming schemes, hierarchies and trust relationships. Since the e-mail system implementation is closely tied to the network operating system implementation, DON-wide collaboration on e-mail system naming and hierarchy is also required to ensure maximum interoperability. Where possible, resource naming should follow the same naming conventions as provided for DNS in Section 6.3.1. The standard fill for the e-mail system user accounts is suggested in Table 6-6.

E-mail System Data Element	Description
Last Name	User's Last Name
First Name	User's First name
Company	Full Name of the Command
Title	Rate and Rank of the User
Department	Command Department or Single Digit Staff Code (e.g., N3)
Office	Title of the Officer, Command or Staff Position, Staff Code

Table 6-6. Standard User Directory Fill

6.5.4 Interoperability with Other E-mail Systems

Because of the dynamic nature and current heterogeneous state of DON electronic messaging and the difficult realities of implementing a single, coordinated messaging solution across the entire DON, it is recommended that SMTP be used as the interconnection backbone.

Through the use of a DON-wide mail switches it should be possible to have a messaging clearinghouse that, coupled with a robust DON wide directory, would be able to process mail for any DON e-mail system in the interim period until DMS becomes operational. This mail switch could also serve as a DMS Multi Function Interpreter (MFI).

6.5.5 Individual's Official E-mail Address

In combination with the master Navy and Marine Corps X.500 directories and the mail switch, the DON directory would be used to dynamically map this address to the multiple changing addresses that users will inevitably have as they change codes or move to other organizations. Note that such a switch system would not preclude organizations from directly interconnecting their respective messaging systems nor would it interfere with the instance where the actual SMTP address of a user is specified.

Each DON user would have at least one SMTP address that follows them independent of the command or organization where they are employed. This address will be referred to as the user's Official Individual Address. The address would take the form of "username@navy.mil" or "username@usmc.mil" and would "follow" its owner throughout his career, independent of duty station.

6.5.6 Display Name

The standard display names for members of your own command should be the following format:
`STAFF CODE – RATE/RANK First Name Last Name`
For example:
`N32 – LT James Jones`

For entries away from the command, the same format should be used except preceded by an abbreviation of the command name.
`COMMAND STAFF CODE – RANK/RATE First Name Last Name`
For example:
`SSN688 OPS LCDR Jim Jones`

For commands where it is inappropriate or confusing to use the staff code to sort display names the following format should be used:
`Last Name First Name (MI) RATE/RANK`
For example:
`Smith, Tom P LCDR`

6.6 Network Utility Services

The following services are needed to monitor, troubleshoot and maintain the network. These services are used by the system administrator and should not be accessible to the operator.

6.6.1 Network Time Service

Time services are established to ensure consistency and accuracy of time and dates across distributed systems. Synchronization is a special problem in networks of multiple hosts because each host has its own clock and its own time reference. Slower clocks continually drift further behind faster clocks. Time skew among networked hosts can cause application delivery problems. For example, a stock trading wire service could be in trouble if brokers in London learned of

deal-making events five minutes after brokers in New York or Hong Kong had already acted. Moreover, time synchronization is critically important to sensor data fusion in C4I and weapon systems.

The DCE Distributed Time Service (DTS) minimizes such situations by synchronizing host clocks in LANs and WANs. Clock synchronization enables distributed applications to determine the sequencing, duration, and scheduling of events, independent of where they occur.

DTS servers synchronize themselves by obtaining time information from all other DTS servers on the LAN. Global servers provide synchronization for servers on extended LANs. DTS alone ensures that DCE hosts share a consistent notion of time. This time, however, is not necessarily the correct time. Servers can be synchronized with external time standards by setting the time manually or by connecting to an external time provider.

The US Naval Observatory is a recognized time reference custodian. DTS uses the Coordinated Universal Time (UTC) standard, which has largely replaced Greenwich Mean Time as a reference. Many standards bodies disseminate UTC by radio, telephone, and satellite. DTS has a Time Provider Interface (TPI) that describes how a time provider process can pass UTC time values to a DTS server and propagate them through a network. The TPI also permits other distributed time services, such as the Network Time Protocol (NTP), to work with DTS. UTC is referenced to a set of atomic clocks and is a proper reference for time synchronization purposes. GMT is referenced to earth's rotation which is several orders of magnitude more variable than the atomic clocks. GMT is adjusted to less than half-second differences to UTC by adding leap seconds either 31 Dec or 30 June as necessary.

Loran and Global Positioning Systems (GPS) receivers provide excellent primary reference and also provide worldwide time services, however, Loran time receivers are a bit more stable because they do not have to contend with selective availability. DTS is transparent to DCE users, but users cannot access DTS directly. Applications can, however, use the time functions available from the DTS API. For example, an application for conference call scheduling can get time zone information from the DTS API to determine the best times to schedule conference calls that span multiple time zones.

Best Practices

For an application that needs the correct time, use either the POSIX.1 time to get a simple scalar with an unknown accuracy or use the DTS API to get the interval time stamp.

Use NTP (RFC1305) and TOG DCE DTS time protocols. TOG DCE DTS supports the synchronization of time with an external time provider, such as Internet time providers, that uses the NTP protocol. Since the NTP is an inherently insecure protocol, it should not be permitted outside of the Zone 4 firewall. If an appropriate time source cannot be found inside of the Zone 4 security boundary, (e.g. DTS) then configuration of a GPS based time source inside of the boundary is appropriate.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	DCE DTS NTP	DCE DTS NTP	DCE DTS NTP	DCE DTS NTP	
Activities, Platforms, Operational Environments		All			

Table 6-7. Network Time Service Recommended Implementations

Notes:

- DCE's Distributed Time Service is a transparent method of obtaining time services that are highly synchronized.
- Network Time Protocol (RFC1305) is a simple method of obtaining time across a network, provided a server is available.

Guidelines

NTP server implementations are publicly available, either bundled in the operating systems or available for download. Many DON combatants have systems onboard which could be used to drive an NTP server; all have a GPS and or Loran receiver with which to cross-check and update. In the right circumstances, it is appropriate for some ships to implement a time-server, and at least one Stratum One clock on NIPRNET can be used as a reference.

6.6.2 System Management Services

System management services permit monitoring, control and management of system objects. The full complement of system management services are covered in Chapter 10. The two primary specifications that support network management are the Simple Network Management Protocol (SNMP) and the Remote Network Monitoring, version 2 (RMON 2).

Best Practices

Use management systems and protocols that minimize non-payload overhead and that can be assembled into an integrated system to control and monitor all aspects of the entire infrastructure from a single workstation.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	SNMPv1 RMON 2 XSM	SNMPv1 RMON 2 XSM	SNMPv1 RMON 2 XSM	SNMPv1 RMON 2 XSM	DMI WBEM
Activities, Platforms, Operational Environments		ITSCs and Shore. Bandwidth consumption must be considered prior to use for Ships, Ground, and Aircraft			

Table 6-8. System Monitoring and Control Recommended Implementation

Notes:

- Simple Network Management Protocol (SMNPv1) has some denial of service security concerns that need to be compensated for by other means.
- Remote Network Monitoring (RMON 2) provides comprehensive system management at or above the network layer.
- Desktop Management Interface (DMI) provides for management of server and personal workstation resources.
- Web Based Enterprise Management (WBEM) is an emerging specification that allows multiple system management access using a Web-based interface.

6.6.3 Remote Access Services

Remote access services are primarily covered by System Management Services and Telnet. Telnet allows remote access of system devices and computers. Its use should normally be disallowed but many legacy applications and systems necessitate the use of Telnet. If used, it should be appropriately proxied and limited only to the necessary personnel.

6.6.4 File Transfer Services

File transfer services let users copy, replicate, or move whole files across a network. TOG and ISO standards help provide standards for this service across a heterogeneous network of conforming systems. In addition, the de facto standard File Transfer Protocol (FTP) is an industry-prevalent mechanism found in most TCP/IP implementations.

Although FTP is a specialized means of transferring files, electronic message handling systems can also be used for transporting files. A standard called Multipurpose Internet Mail Extensions (MIME), which has emerged from the Internet mail protocol (SMTP), permits various file types to be transferred as attachments to messages. All mail systems have limits on the size of files they can transfer; some are as few as 32 KB (kilobytes).

Most network operating systems have file transfer capabilities integrated into their file systems that make network file transfer as easy as dragging and dropping files from one folder to another. Rarely are these proprietary systems useful outside their local implementation domain and those

that have that functionality tend to pose unsatisfactory security risks. Moreover, these systems are notoriously inefficient from a networking standpoint, especially over low bandwidth channels.

The use of the Hypertext Transfer Protocol (HTTP) continues to open up new opportunities to construct file transfer systems across multiple networking environments and systems. Coupled with file compression and "push-technology", this de facto, open standard may also provide file transfer capabilities to bandwidth challenged environments. As HTTP continues to become embedded in desktop and server operating systems, use of its file transfer mechanism is likely to increase.

Current tools and methods assume that any encryption requirements are handled before and after file transfer. Future implementations are expected to integrate encryption support or be compatible with a Public Key Infrastructure (PKI) implementation of X.500/509.

Best Practices

Select file transfer systems that conform to open standards and promote interoperability. The electronic messaging method of file transfer should only be used for small files (already compressed using ZIP), ideally less than 5 MB. Files larger than 5 MB should be transferred using the Web Drop and Pickup Service (Section 6.2.8).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Proprietary file transfer systems	HTTP FTP MIME RFC 1521 S/MIME RFC2312	HTTP FTP MIME RFC 1521 S/MIME RFC2312	HTTP FTP MIME RFC 1521 S/MIME RFC2312	HTTP FTP MIME RFC 1521 S/MIME RFC2312	
Activities, Platforms, Operational Environments		All			

Table 6-9. File Transfer Service Recommended Implementations

Notes:

- Use file transfer system implementations that are based on the Internet Protocol (IP) standard
- SHTTP is a more secure version of HTTP that provides a basic level of encryption of data for data traveling between the client and server

6.6.5 Electronic Dialog

Along with Network News Service (Section 6.8), electronic dialog can be accomplished using Internet Relay Chat (IRC). There are many applications for a running type dialog such as system troubleshooting over small bandwidth links.

6.7 Web Services

A "web" is a collection of servers on a network that communicate with web browsers using the Hypertext Transport Protocol (HTTP). The most famous web is the World Wide Web, which is the collection of web servers publicly available on the Internet. The browser sends an HTTP request to a web server for a Hypertext Markup Language (HTML) document. After receiving the document, the browser displays it to the user. An HTML document can contain text, graphics, and links to other documents or to different sections of the current document in the form of Uniform Resource Locators (URLs). An HTML file can also contain embedded within it audio files, video files, 3D graphics, Virtual Reality Modeling Language (VRML), or other document types. Further, an HTML document can contain its own locally executed instructions (scripts) for simple activities or full-blown applications in the form of Java applets or ActiveX objects. A link can refer to a Common Gateway Interface (CGI) which supports additional functionality on the server side of the connection, e.g., a database interface or added security processing.

6.7.1 Web Servers

A web server is any computer on a network that is running Hypertext Transfer Protocol (HTTP) server software. HTTP can be used to move any kind of data over a TCP/IP network between a web server and a web browser (client). HTTP is a transaction-oriented client/server protocol.

Even though there are many document formats/protocols listed in Section 6.7.2 (Web Browser), the web server, which only needs to speak HTTP is serving them all. HTTP is the dominant protocol (majority of network traffic) on the Internet, as well as on many dedicated DoD networks.

In addition to serving up HTML pages to the clients, the HTTP server must support Common Gateway Interfaces (CGI). CGI is an Application Program Interface (API) that supports server side processing, i.e., the execution of applications on the web server or another machine for which the web server is acting as a front-end. Examples of server side applications include processing HTML forms, dynamic document generation, and providing access to database servers. CGI scripts are typically written using UNIX shell scripts, Perl, TCL/TK or C, but can be written in almost any programming language (see Chapter 9 for development tools and languages).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	HTTP 1.0 SSL	HTTPv1.1 SSL	HTTP-NG SSL	HTTP-NG SSL	
Activities, Platforms, Operational Environments		All			

Table 6-10. Web Service Recommended Implementations

Notes:

- HTTP is the standard of the Internet Engineering Task Force, the current release version is HTTP 1.0, however, HTTP version 1.1 is IETF proposed standard RFC 2068 and is currently undergoing public review.
- HTTP 1.1 is designed to bring about significant performance gains through support for persistent connections and pipelining for much more efficient use of TCP networks, continued extension of the caching model and support for multi-homing servers (allowing a single web server to serve multiple web sites each with their own unique address). Improvements in HTTP 1.1 are limited due to the requirement for backwards compatibility with HTTP 1.0.
- HTTP-Next Generation (HTTP-NG) is an on-going effort to redesign the HTTP protocol for greatly increased efficiencies.
- Secure Sockets Layer (SSL) is an extension to HTTP that provides for user authentication, added privacy and assurances of data integrity.

Guidelines

A web server is a very public resource that must be well maintained with regard to security vulnerabilities to prevent compromise resulting from publication of erroneous data or denial of service.

There are a number of tools that make administering a web server significantly easier, see Section 6.7.3, WWW Utilities, for more information on these.

Web servers are often sold as suites that can include a message (e-mail) server, a directory server (typically LDAP), a data push content server, a streaming audio/video server, and text search services. Standards and functionality for these functions are addressed elsewhere in this document. Significant cost savings on purchase price and integration can be afforded by buying bundled server suites.

Network performance can be significantly affected by the use of effective caching schemes between the client and server to prevent the repeated download of pages from the server that exist on the client cache and have not changed.

6.7.2 Web Browsers

The web browser or client is primarily the local user's viewer for documents provided by the HTTP server. The browser is now evolving to be the main, or sole element of the presentation

layer of many system architectures. The web browser provides an easy-to-manage, universal client interface for display of text, graphics, multimedia, and forms-based data. The browser's native data display capabilities can be extended through the use of external "helper" applications or Java applets to support graphics-intensive or real-time data display requirements.

The web browser's native language is Hypertext Markup Language (HTML). HTML is a platform independent "tagged" language that is both human and machine readable and can be transmitted as straight ASCII data. The current version includes support for advanced forms, in-line frames, enhanced tables, support for objects and scripts, style sheets and more.

A key browser technology that was originally handled by "helper" applications, but which is now being built into browsers is Virtual Reality Modeling Language (VRML). VRML will realize increasing use for 3D user interfaces and has great potential for military applications.

Another browser extension with excellent military potential is variable resolution still images. This technology delivers higher-resolution images only as they are needed, minimizing network bandwidth demands while enabling a user to pan and zoom on an image. Use of this technology can also greatly improve print quality by downloading a higher resolution version of the image when printing (computer screen display is at 72 dots per inch while printers typically require 150 to 300 dots per inch). The initial commercial implementation of this technology is FlashPix, an effort by Kodak, Hewlett-Packard, Live Picture and Microsoft. FlashPix is built on top of the new Internet Imaging Protocol (IIP) - defined by Hewlett-Packard and endorsed by Netscape and Microsoft. IIF enables a plug-in, applet or helper application to interactively request image and property data from a web server. For example, a client can request just a section of an image. IIF was designed for FlashPix but it works with Graphics Interchange Format (GIF) and Joint Photographic Experts Group (JPEG) images also.

6.7.2.1 Evolution of HTML

There are many initiatives under way to extend or replace HTML as the demands being placed on the web interface grow beyond the display of simply formatted static documents. These initiatives are under the auspices of the World Wide Web Consortium - the industry/education partnership that controls most WWW standards.

The need for more complex document formatting led to the development of Cascading Style Sheets (CSS). CSS allows a page author to specify a much more precise document formatting template that is automatically applied to the entire document instead of requiring manually set display attributes for every element of the document (http://www.w3.org/areas.htm).

The desire for more interactive web pages led to the creation of Dynamic HTML. Dynamic HTML is a set of technologies that expose HTML attributes as properties that can be manipulated by scripts. DHTML is complex to produce manually but there are increasing numbers of HTML editors that support it. Using DHTML is made more difficult by the differing implementations on Netscape Navigator and Microsoft Internet Explorer.

DHTML is built on top of the Document Object Model (DOM) which is "a platform- and language-neutral interface that will allow programs and scripts to dynamically access and update the content, structure and style of documents" (http://www.w3.org/areas.htm).

The eXtensible Markup Language (XML) is the proposed ‘follow-on’ to HTML. XML is based on the Standard Generalized Markup Language (SGML), ISO Standard 8879, tailored for the

WWW. "XML is primarily intended to meet the requirements of large-scale Web content providers for industry-specific markup, vendor-neutral data exchange, media-independent publishing, one-on-one marketing, workflow management in collaborative authoring environments, and the processing of Web documents by intelligent agents" (http://www.w3.org/Press/XML-PR.html).

The major key feature found in XML is that it allows publishers to define their own markup language using application specific meanings. This would enable an author to build mathematical equation structure; automatic database updates with schemas intact; integrated meta information system structures; XML protocol enabled selectively address and download of portions of XML documents; and new animation, scripting, object model, style sheets, automation, and printing functionality.

Channel Definition Format (CDF) is XML extension proposed by Microsoft to define content and format for pushed (webcast) data.

6.7.2.2 Procedural Extensions

HTML is not designed to support procedural capabilities (i.e. the ability to execute application code or carry out some procedure). However, web pages can add procedural capabilities – primarily as extensions to the user interface - via client-side scripting or server-side scripting via embedded application parts or applets. The use of these proprietary extensions should be carefully controlled and the web development should adhere to HTML standards to ensure cross platform browser compatibility.

Client-side scripting includes small sections of program code stored in HTML pages that are interpreted by the client when the page is loaded. Client-side scripting is done in JavaScript (based loosely on Java) or VBScript (based on Visual Basic).

Server-side scripting is discussed in Section 6.7.1 (Web Servers).

Application parts are either ActiveX parts or Java applets. ActiveX parts are embeddable program objects, typically written in Visual Basic, but they can be in C or Java. Java is an object-oriented programming language based on the C programming language. Java can be used to program either conventional stand-alone applications or small downloadable applications called "applets." The partially compiled source code (called bytecode) for an applet is embedded in the HTML document. When the document is downloaded from the web server, the Java bytecode is automatically executed by the system or browser's Java Virtual Machine.

6.7.2.3 Extension of the Web Browser as an Application Interface

In the personal computer world, there is an increasing blurring of the lines between the browser and the operating system top-level interface or "desktop." Microsoft, in particular, is pushing the total integration of Internet Explorer with the Windows95 and Windows NT desktop through their Active Desktop product. Regardless of how that effort turns out, the browser will provide building blocks for developers to easily create user interface functionality. The various user interface and control elements of the web browsers are being turned into programmable objects. For example, both Internet Explorer and Netscape Navigator include e-mail programs that support HTML formatted electronic mail by embedding the browser's display functionality in the mail application. This technical direction will be enhanced with the release of web browsers that are written entirely in Java.

Netscape has created a Resource Definition Framework (RDF) that allows for the creation of a metadata layer of the underlying data stores of Netscape Communicator - allowing users to customize the user interface. RDF is based on the eXtensible Markup Language (XML). Netscape also plans to expose the Communicator APIs as JavaBeans and scriptable components, allowing developers to create applications built on top of these capabilities. Netscape will also make available to developers a new rendering engine (code-named Gemini) that supports HTML, XML and other formats that developers can embed directly into their own applications.

There is currently no standard set of APIs or object interfaces for manipulating all browsers.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	HTML 4.0	HTML			XML
	Java	VRML			PNG
	JavaScript				PICS
	VRML 2.0				RDF
	Quicktime VR				SMIL
	Quicktime				RTP
	AVI (MPEG-4)				RTSP
	SSL				IIP/Flashpix
					SETP
					DOM CSSI
					CDF
Activities, Platforms, Operational Environments		All			

Table 6-11. Web Client Recommended Implementations

Notes:

- Several of these standards duplicate standards included in Section 6.3.1 (Web Servers) because the web server and the web client must speak the same protocol for those protocols involved in communication between the client and server.
- W3C released HTML 4.0 as a "recommendation" on 12/18/97 (http://www.w3.org/Press/HTML4-REC, 1/11/98, 9:02PM). There will be a transition from the current HTML 3.2 standard to HTML 4.0. Browsers and development tools that support HTML 4.0 are currently available, however all features of HTML 4.0 are not supported by all web browsers.
- eXtensible Markup Language (XML) 1.0 is a "proposed recommendation" being voted on by W3C membership for consideration as a "Recommendation."

- Java applets are supported by both leading browsers (Navigator and IE); ActiveX support may not be available on all platforms. Java applets should be written in "100% Pure" Java code - not using Microsoft specific extensions.
- JavaScript is supported by both leading browsers (Navigator and IE); VBScript is only supported by Microsoft.
- VRML 2.0 supports 3-D rendering of navigable spaces plus encapsulation of images, animation and audio. VRML supports "hot spots" - allowing a developer to embed hyperlinks to other HTML or VRML documents or embed other programming languages so objects can be assigned behaviors.
- QuicktimeVR supports 3D navigable spaces that are composed of 360 degree panoramic photos which can be navigated similar to VRML.
- Quicktime is a multimedia data format for synchronized media (sound and video) that is cross-platform and popular.
- AVI - digitized video data format popular in the personal computer world.
- Portable Network Graphics (PNG) - W3C initiative to develop an improved bitmap graphics format that addresses limitations of current formats (http://www.w3.org/areas.htm).
- Platform for Internet Content Selection (PICS) - W3C specification provides for labeling of web site content. While this is primarily used today to provide access restrictions for children on the Internet, there are potential applications for this technology on Navy sites (http://www.w3.org/areas.htm).
- Resource Definition Framework (RDF) - PICS is at the heart of an expanded "metadata" effort at the W3C to provide a standard way to describe the properties of web pages - including providing data for access controls, copyright restrictions, additional security functionality and improved content indexing (http://www.w3.org/Metadata/activity.html).
- Synchronized Multimedia Integration Language (SMIL) is a W3C initiative to language for controlling "continuous multimedia presentations" where audio, video, text and images must be presented in a synchronized relationship. The first public draft for SMIL was released by the W3C in November 1977 (http://www.w3.org/audiovideo/activity.html).
- Real Time Transport Protocol (RTP) - protocol for streaming data (audio and video) applications developed by the Internet Engineering Task Force (IETF). (http://www.w3.org/audiovideo/activity.html. Also see http://www.ietf.cnri.reston.va.us/home.html for more information.)
- Real-Time Streaming Protocol (RTSP) - protocol under development by the IETF, that builds on HTTP technology (caching, authentication, encryption), for streaming data (audio and video) applications (http://www.w3.org/audiovideo/activity.html. Also see http://www.ietf.cnri.reston.va.us/home.html for more information.)
- Internet Imaging Protocol (IIP)
- Live Picture Inc., FlashPix image format, Realspace Image Server, FlashPix plug-in
- FlashPix technology was developed jointly by Kodak, HP, Live Picture and Microsoft
- Secure Sockets Layer (SSL) is an extension to HTTP that provides for user authentication, added privacy and assurances of data integrity
- Secure Electronic Transaction Protocol (SETP) - developmental security protocol designed to enhance the security of digital commerce transactions, supported by both Netscape and Microsoft
- Document Object Model - "a platform- and language-neutral interface that will allow programs and scripts to dynamically access and update the content, structure and style of documents. The document can be further processed and the results of the processing can

be incorporated back into the presented page." http://www.w3.org/areas.htm (11 January 1998)
- Cascading Style Sheets Level 1 (CSS1) is W3C recommendation
- Channel Definition Format (CDF) is XML extension proposed by Microsoft to define content and format for pushed (webcast) data. It has not yet been accepted by any standards organization.

Guidelines

Use of formats other than HTML for data distribution (i.e. Portable Document Format (PDF), Java) hides data from search engines and inconveniences users who have to wait for a plug-in or helper application to download and/or launch or wait for the Java applet to launch before they can view the document. Packaging data in these formats also discourages its reuse.

With the aggressive addition of new web browser features by both Netscape and Microsoft, adherence to the HTML standard provides the only guarantee of compatibility with all web browsers. Features beyond the current HTML standard should be used only when the user is certain that both vendors support the new feature. Even adherence to the HTML standard is not a guarantee that all users will be able to access all the functionality of a web site. A site developer must ensure that the entire target audience has, or will, upgrade their browser to the version that supports the current HTML standard or added feature before fielding new HTML features.

Both Netscape and Microsoft make their browsers available as part of a larger suite of integrated applications. If an organization has already paid a license for this suite of software and is going to install the shared code necessary to run the web browser, there are cost efficiencies in using the remaining elements of the suite. This should be taken into consideration when evaluating products for e-mail clients, newsgroup readers, data push solutions, HTML editors, directory services clients and collaboration tools. If the bundled solutions are not to be used by the organization then steps should be taken to prevent their use as an alternate to the approved standard application.

6.7.2.4 Browser Security

In addition to the security protocols identified in the Recommended Implementation section, here are some other general web browser security notes.

The security of Java applets is addressed by the “sandbox” restrictions built into the Java language.

A web browser gives the end user the ability to download and open files directly in an external application (for example Microsoft Word). Most current virus protection software will not catch an infected document that is not saved to the disk first and then opened by an application. There are commercial products that claim to support this, either web browser anti-virus plug-ins or continuous background virus checkers that are supposed to intercept files once downloaded. Web technologies and products should be subject to careful security evaluation prior to deployment and tight configuration control once deployed.

The use of digital certificates is a key technology for positively identifying a web browser user to a web server. Certificates surpass passwords in providing strong security by authenticating identity, verifying message and content integrity, ensuring privacy, authorizing access, authorizing transactions, and supporting non-repudiation. Digital certificates are discussed in more detail in Section 3.5, Public Key Infrastructure.

6.7.3 Web Utilities

There are necessary capabilities beyond web servers and browsers that make it possible for the web to work. These include HTML editors, web site content management tools, web site scripting tools and languages, site usage tracking tools, web server management tools, site watchers and site grabbers.

6.7.3.1 HTML Editors

There are a large variety of What-You-See-Is-What-You-Get (WYSIWYG) web page editor applications available with the goal of allowing any user to created HTML documents without having to actually write HTML. Each of the leading browser packages include a basic HTML editor (Microsoft FrontPage Light, Netscape Composer), however there are other products available which provide additional functionality. Any tool selected should support:

- WYSIWYG frames page editing
- basic image manipulation (resize, brightness and contrast adjustment, transparency)
- image map creation (definition of hotspots and associated URLs)
- easy table creation
- linkage for document preview in a web browser
- support for automatic generation of navigation bars and other shared page elements
- the ability to apply a consistent style or "look and feel" to a collection of web pages

Any tool selected should also support new features as they are added to the appropriate web standards and as the leading browsers implement them. It is worth noting that many (today), and eventually most (soon) office productivity applications have an "export to HTML" capability, making them advanced HTML editors of a sort.

6.7.3.2 Web Site Content Management

While most any user is capable of generating HTML documents, most are not capable of managing a web server. The most frequent day-to-day activity involved in web server or "site management" is updating the content of the server. There is now a class of tools typically referred to as "site managers" that provide a graphical user interface for adding and deleting files from web sites, moving elements of the site around (and automatically updating the changed links), link validation (to find broken links), and migration of sites from one server to another.

6.7.3.3 Web Site Scripting Tools and Languages

Web pages can be extended to support a richer user interface or local application functionality through the use of procedural languages. There are two languages that can be applied at the document level (included in the document and interpreted at run-time) - JavaScript and VBScript. Other languages can be used to create application parts that are incorporated into a web page. These are typically implemented as Java applets or ActiveX parts. This is an area where there is conflict between the two leading browser vendors (Netscape and Microsoft) and not every browser supports all these technologies.

6.7.3.4 Site Usage Tracking

These are tools that allow non-real-time data analysis on HTTP server logs to identify who is accessing a web server and what sections of the server are being accessed.

6.7.3.5 Web Server Management

There are many functions that a web server system administrator needs to be able to perform. There should be some alert mechanism to make the administrator aware when web servers fail or reach specified traffic thresholds. For a heavily trafficked site, applying software tools that balance web server load across several web servers is a key approach to maintaining reasonable response times for users. The ability to test web server performance, to analyze traffic on local network segments to identify choke points, and the ability to monitor server activity in real time are all useful system administrator functions supported by these tools. Finally, the ability to identify all web servers on an Intranet is useful - especially for finding unauthorized web servers.

6.7.3.6 Web Watchers

These are tools that are typically applied at the individual user level to allow them to "register" pages on servers that they want to be notified of updates. Typically, when a page on a server being "watched" is updated, an e-mail is sent to the user announcing the update. This functionality can be provided by the site being monitored, but more frequently needs to be provided by a tool running locally. An ability to set up user bookmarks as "subscriptions" is included in Internet Explorer 4.0 and will probably migrate to other browsers. The subscribed sites are periodically checked for updates and the user can be notified through a change in the visual representation of the site's bookmark.

6.7.3.7 Site Grabbers

These are tools that are typically applied at the user level to simplify the process of downloading the multiple data elements (HTML and GIF images) that make up a document on a web server. These tools can also be applied at a command level to mirror outside sites - to speed access, ensure availability or to meet security constraints. The end user specifies what sites to download, how frequently and how many levels deep within the site to download and if the download should include links to sites outside the target site. Some tools also allow the user to specify the maximum amount of disk space a downloaded site snapshot can take up. Properly implemented, the site browser will go first to the local snapshot of an external site and see if the local information is current, before going out over the (typically slower) network to contact the site itself.

Best Practices

To be determined.

Recommended Implementations

There are no standards specific to these tools. The tools need to support the standards called out in the Web Server and Web Browser sections of this document. As preferences emerge, they will be provided in future DON ITSG releases.

6.7.4 Data Search and Retrieval

The web browser is increasingly becoming the standard or preferred interface for information presentation. Associated with that function, the web also serves as the interface and infrastructure for a wide range of data search and retrieval technologies that make data, especially from legacy systems, available to the end user.

These capabilities are typically made available through the use of a three tier or three layer architecture where the web browser is tier one, the HTTP (web) server and its associated applications (through CGIs) are tier two, and the database or other back-end server is tier three.

Data search and retrieval functionality can be broken down into three main areas - database access, web search engines and text search.

6.7.4.1 Database Access

Some experts predict that within two years, 80% of database queries will be over the web. The web typically provides easier to use interfaces at lower costs to an expanded user base. Database access is typically provided by using the web browser as the user interface which talks through the web server to an application called a "middleware" package that in turn talks to the database server. The goal of the middleware package is to hide the differences and details of the interface to the various database servers from the developer who is setting up the web interface to the database. The user interface for querying the database is almost always via a form the user fills in with search terms, and the results are normally either displayed in a form or as lists of links the user can select to get more detailed information.

6.7.4.2 Web Search Engines

Any user who has been on the World Wide Web should be familiar with the services provided by commercial web search engines like Yahoo! and AltaVista. This same functionality is available for implementation on Intranets. The end user provides one or more keywords or a phrase to search on and the search engine returns a list of sites that match the query. Various search engines support more complex queries, ranking the results based on the quality of the match to the query and various approaches to collecting and indexing information about sites.

Web search functionality can be divided into two main classes – web directories that provide an indexed structured view of sites based on site keywords and selected contents (like Yahoo!) and search engines that index the full content of web sites (as represented by AltaVista).

6.7.4.3 Text Search

Full-text and attribute-based searches support creation indexes of intranet and Internet information with browsable category tree interface. This is different than an unstructured text archive/search engine (Memex, Topic, etc.), that is also an essential function (especially for dealing with message traffic) that can typically be provided through a web interface. This information can be indexed in many native application formats (Office) as well as text and HTML. “Robots” are agents that traverse the net and collect information, submit to the search server for indexing and categorization, and then serve up to users (through search/browse managers). Live query can be conducted though single and multi-field keyword searches. There are no standards for any of this (other than HTML enabled mail for delivery of newsletters that contain links/URLs).

Recommended Implementations

- Any database middleware packages should support the ANSI SQL query language standard. Microsoft's Open Database Connectivity (ODBC) is a de facto standard for vendor-independent database access and should also be supported.

- IBM, Oracle, Sybase, Informix and Microsoft all have either middleware applications that talk to their database servers or direct web access to their database servers. There are also a large number of third-party middleware applications that interface to database servers from multiple vendors.
- There are no standards that are applicable to web search engines.
- There are no standards that are applicable to text search engines.

Implementation Concerns

- Internet or Intranet search engines are not particularly intelligent. If you don't tell them what your site is about they will just grab your site's home page and characterize your site based on that. If you want to control how your site is profiled you can use "meta" tags on your sites home page html document. For example the two meta entries:
  <META name="description" content="CINCPAC J-3 Home Page">

  <META name="keywords" content="CINCPAC, joint, planning, operations">

  tell the web search engines that your page should be described as the "CINCPAC J-3 Home Page" and that it has to do with CINCPAC's joint planning and operations (those will be the keywords that a user's search will hit on).

- Avoid storing content in a non-indexable format (i.e. PDF)[10].
- Providing explicit notification to index engines to ensure proper or desired information is conveyed to the network public
- If you have a web server that you don't want to have show up in the web search engines or parts of the web site that you don't want indexed, you can create a "robots.txt" file that most of the search engines web crawler robots will respect. The format looks like this:
  #Sample anti-robot file

  User-agent: *

  Disallow: /

  To prevent all indexing

  #Sample anti-robot file

  User-agent: *

  Disallow: /temp

  Disallow:/test

- To prevent indexing of files in the "temp" and "test" directories of your site.

6.7.5 Data Push

A user with a web browser is engaging in a data pull activity, he or she is actively selecting sites and pages of interest and manually navigating to those pages to review the information there. An

[10] PDF, however, makes large volumes of information very portable. This portability versus PDF's inherent lack of "indexability" should be weighed. Often it is little additional effort to create both an HTML and PDF version of a document to achieve both indexability and portability.

alternate mode of information transfer that can be implemented using web technologies is data push. In a data push mode of operation the user has a choice of broadcast channels to choose from and subscribe to. During the subscription process the user decides how often they want the information updated and how the information is to be displayed. Information display can range from small scrolling marquee windows on the desktop, to traditional web browser pages, to dynamic screen savers.

There are currently three popular data push solutions that users may have experience with - PointCast, Netscape's Netcaster, Microsoft's Active Channels. Each of these solutions uses a different technology and is incompatible with the others. The typical use for these push products has been to deliver news and entertainment information from traditional sources (major network news organizations and magazines) to the desktop. The more interesting application for Navy and Marine Corps use is using data push as a way to deliver intelligence updates, morning briefs, general interest administrative material or critical real-time data or alerts. Each of the major commercial push solutions has a "push server" technology that can be adopted by an organization to deliver its own channelized information.

Recommended Implementations

There are currently no standards to govern push technology. Some solutions deliver information in straight HTML format, so the normal web browser and web server standards apply. Microsoft has proposed a new standard - the Content Definition Format (CDF) - for delivery of push data, but no standard body has adopted this proposed standard.

The World Wide Web Consortium (W3C) has released the first public working draft of Synchronized Multimedia Integration Language (SMIL). SMIL is a language that enables authors to bring television-like audio-video content to the Web over low-bandwidth connections. SMIL has the potential to make it easy to produce channels of push content that are much more dynamic than the current text and image pages typically delivered.

Guidelines

Because pushed information is downloaded to the user's system, potentially with frequent updates whether the user is there and reading it or not, pushed information can consume excessive network bandwidth. Organizations can control bandwidth utilization by restricting the number of push channels that are available and implementing local intermediate servers that cache the updates for all the channels instead of downloading the data directly to the user's desktop. Unfortunately, not all push deliver technologies support either of these techniques.

There is momentum behind Microsoft's CDF proposal. However, to use CDF, you have to insert a separate stream of text into your document, in a block of XML (extensible markup language) instead of HTML. That means that each hyperlink on your page has to be coded twice — once in HTML for Web browsers, and again in XML for push clients. XML is the proposed successor to HTML and someday this parallel data format issue will probably go away. In addition, the site designer has to create a separate, master CDF file that contains additional information about the site.

6.8 Network News Service

Internet/Intranet news is the most basic form of smart data pull. The user has a "net news" client program that connects to a "news server". The user then selects "newsgroups" to subscribe to and the client interface shows the active messages in each subscribed to newsgroup and allows the user to retrieve and read the contents of any news "posting" or message. Network News Transfer Protocol (NNTP) specifies the language for communication between the local news server and news clients. NNTP also specifies the language for communication between news servers.

Network news provides a more efficient alternative to e-mail mailing lists. News implementations allow users to pull only the information they are interested in when they are interested in it. News implementations also eliminate the workload of maintaining mailing lists.

The NNTP standard was defined in 1986, and it has stood the test of time very well. NNTP is an open protocol that does not restrict the content of news messages so it has allowed for the evolution of news content from plain text to richer data formats including binary data (typically pictures) and HTML. Support for news content beyond plain text is dependent on the user's client news reader software and the client capabilities of the intended audience must be considered before employing any rich data formats.

There are desirable features for a network news implementation that were not included in the original NNTP standard. These additional features have been added to the basic NNTP functionality by specific vendors. These add-on features include the ability to perform a text search across multiple newsgroups on the server and user-level access restrictions. While useful, these features do not comply with the standard and should generally be avoided.

Best Practices

Use NNTP for network news service. Use network news as the primary means of posting and dialog of information to groups, particularly if the information is not urgent. It can be particularly useful to offload “unofficial” messages of general interest such as bake sales and car washes from the e-mail system. It is also useful, however, to communicate and urgent and important information on a continuing basis to a large number of subscribers on a broadcast or dialog basis.

Recommended Implementation

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	NNTP	NNTP	NNTP	NNTP	
Activities, Platforms, Operational Environments		All			

Table 6-12. Network News Standard

The NNTP standard is defined in Request for Comment (RFC) 977 titled Network News Transfer Protocol and dated February, 1986. The introductory paragraph describes NNTP as "a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the Internet community. NNTP is designed so that news articles are stored in a central database allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided."

NNTP 1.5 is the "reference" implementation of the NNTP protocol, but there are many other valid implementations of NNTP compliant news servers and clients available as either free or commercial software.

6.9 References

6.9.1 Standards and Specifications Resources

Domain Name System (DNS)

The DNS provides the service of translating between host names and IP addresses. DNS uses TCP/UDP as a transport service when used in conjunction with other services. See IAB Standard 13, as profiled by MIL-STD-2045-17505

Department of Defense (DOD) MIL-STD-2045-17505: “Information Technology DOD Standardized Profile Internet Domain Name System (DNS);” 29 July 1994; http://www-library.itsi.disa.mil/org/mil_std/ms2045_17505.html (24 May 1998)

Mockapetris (USC ISI); “Domain Names – Implementation And Specification”; (RFC 1035); November 1987; ftp://ftp.isi.edu/in-notes/rfc1035.txt (24 May 1998)

The Open Group (TOG); XFN Specification: “Federated Naming;” July 1995; http://www.opengroup.org/publications/catalog/c403.htm (24 May 1998)
Lottor (SRI Intl.); “Domain Names – Concepts and Facilities” (RFC 1033); November 1987; ftp://ftp.isi.edu/in-notes/rfc1033.txt (24 May 1998)

Directory Services

International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. X.500 also provides security services used by DMS-compliant X.400 implementations.

Kille (Isode Ltd.), Wahl (Critical Angle Inc.), Grimstad, Huber, Sataluri (AT&T); “Using Domains in LDAP/X.500 Distinguished Names” (RFC 2247); January 1998; ftp://ftp.isi.edu/in-notes/rfc2247.txt (24 May 1998)

Electronic Messaging

Hardcastle-Kille (University College London); “Mapping between X.400(1988) / ISO 10021 and RFC 822” (RFC 1327) [See “Crocker”]; May 1992; ftp://ftp.isi.edu/in-notes/rfc1327.txt (24 May 1998)

Crocker (Univ. of Delaware); “Standard for the Format of ARPA Internet Text Messages:” (RFC 822) 13 August 1982; ftp://ftp.isi.edu/in-notes/rfc822.txt (24 May 1998)

Rose (Performance Systems Intl.); “Post Office Protocol – Version 3” (RFC 1225); May 1991; ftp://ftp.isi.edu/in-notes/rfc1225.txt (24 May 1998)

Crispin (Univ. of Washington); “Distributed Electronic Mail Models In IMAP4” (RFC1733); December 1994; ftp://ftp.isi.edu/in-notes/rfc1733.txt (24 May 1998)

International Telecommunications Union – Telecommunications (ITU-T); X.400/F.400 Standard: “Message Handling: System and Service Overview;” July 1996

The standard for electronic mail is the Defense Messaging System (DMS) X.400-based suite of military messaging standards as defined in Allied Communication Publication (ACP) 123 and ACP 123 U.S. Supplement No. 1. The U.S. Supplement annexes contain standards profiles for the definition of the DMS “Business Class Messaging“ (P772) capability; additional standards definition; and DMS use of the Message Security Protocol (MSP)

Joint Staff; Allied Communication Publication (ACP) 123 and ACP 123 Supplement 1: “Common Messaging Strategy and Procedures”; 1 January 1995; http://dmsweb.crcc.disa.mil/dmspub/ACP123%20Mainbody.htm (24 May 1998)

Betanov; “Introduction to X.400”; December 1992, Artech House, Inc.; Norwood, MA;

File Transfer

Basic file transfer shall be accomplished using File Transfer Protocol (FTP). FTP provides a reliable, file transfer service for text or binary files. FTP uses TCP as a transport service. See IAB Standard 9, as profiled by MIL-STD-2045-17504

Department of Defense (DOD) MIL-STD-2045-17504: “Information Technology DOD Standardized Profile Internet File Transfer Profile for DOD Communications;” 29 July 1994; http://www-library.itsi.disa.mil/org/mil_std/ms2045_17504.html (24 May 1998)

Internet Activities Board (IAB); “Protocol Standard For A NetBIOS Service On A TCP/UDP Transport: Concepts And Methods;” (RFC 1001) March 1987; ftp://ftp.isi.edu/in-notes/rfc1001.txt; (24 May 1998)

Auerbach (Epilog Technology Corp.); “Protocol Standard For A NetBIOS Service On A TCP/UDP Transport: Detailed Specifications; (RFC 1002) March 1987; ftp://ftp.isi.edu/in-notes/rfc1002.txt (23 May 1998)

Jurg (SurfNet); “Requirements for IP Version 4 Routers” (RFC 1684); August 1994; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1684.txt (23 May 1998)